ia – inr

icmp

To configure access rules for ICMP traffic that terminates at the Secure Firewall ASA interface, use the **icmp** command. To remove the configuration, use the **no** form of this command.

icmp { **permit** | **deny** } *ip_address net_mask* [*icmp_type*] *if_name*
no icmp { **permit** | **deny** } *ip_address net_mask* [*icmp_type*] *if_name*

Syntax Description

deny	Deny access if the conditions are matched.
icmp_type	(Optional) ICMP message type (see Table 1-1).
if_name	The interface name.
ip_address	The IP address of the host sending ICMP messages to the interface.
net_mask	The network mask to be applied to the IP address of the host.
permit	Permit access if the conditions are matched.

Command Default

The default behavior of the ASA is to allow all ICMP traffic to the ASA interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **icmp** command controls ICMP traffic that terminates on any ASA interface. If no ICMP control list is configured, then the ASA accepts all ICMP traffic that terminates at any interface, including the outside interface. However, by default, the ASA does not respond to ICMP echo requests directed to a broadcast address.

The ASA only responds to ICMP traffic sent to the interface that traffic comes in on; you cannot send ICMP traffic through an interface to a far interface.

VPN access to an interface other than the one from which you entered the ASA is not supported. For example, if your VPN access is located on the outside interface, you can only initiate a connection directly to the outside interface. You should enable VPN on the directly accessible interface of the ASA and use name resolution so that you don’t have to remember multiple addresses.

The icmp deny command disables pinging to an interface, and the icmp permit command enables pinging to an interface. With pinging disabled, the ASA cannot be detected on the network. This is also referred to as configurable proxy pinging.

Use the access-list extended or access-group command for ICMP traffic that is routed through the ASA for destinations on a protected interface.

We recommend that you grant permission for the ICMP unreachable message type (type 3). Denying ICMP unreachable messages disables ICMP path MTU discovery, which can halt IPsec and PPTP traffic. See RFC 1195 and RFC 1435 for details about path MTU discovery.

If an ICMP control list is configured for an interface, then the ASA first matches the specified ICMP traffic and then applies an implicit deny for all other ICMP traffic on that interface. That is, if the first matched entry is a permit entry, the ICMP packet continues to be processed. If the first matched entry is a deny entry or an entry is not matched, the ASA discards the ICMP packet and generates a syslog message. An exception is when an ICMP control list is not configured; in that case, a permit statement is assumed.

The following table lists the supported ICMP type values.

Table 1: ICMP Types and Literals

ICMP Type	Literal	Description
0	echo-reply	The echo reply is the response to an echo request to indicate successful communication.
3	unreachable	The device could not deliver a package to the final desination.
8	echo	The echo message that carries the address of the source. This address is the destination for the echo-reply message.
11	time-exceeded	During processing of a package, the device identifies the Time-To-Live value equal to zero and therefore the package is discarded.

Examples

The following example denies all ping requests and all incoming ICMP connections in general, except for unreachable messages, at the outside interface:

```
ciscoasa(config)# icmp permit any unreachable outside
```

Continue entering the **icmp deny any** *interface* command for each additional interface on which you want to deny ICMP traffic.

The following example permits host 172.16.2.15 or hosts on subnet 172.22.1.0/16 to ping the outside interface:

```
ciscoasa(config)# icmp permit host 172.16.2.15 echo outside
ciscoasa(config)# icmp permit 172.22.1.0 255.255.0.0 echo outside
ciscoasa(config)# icmp permit any unreachable outside
```

Related Commands

Commands	Description
clear configure icmp	Clears the ICMP configuration.

Commands	Description
debug icmp	Enables the display of debug information for ICMP.
show icmp	Displays ICMP configuration.
timeout icmp	Configures the idle timeout for ICMP.

icmp-object

To add ICMP types to an ICMP object group, use the icmp-object command in icmp-type configuration mode. To remove ICMP types, use the **no** form of this command.

icmp-object*icmp_type*
no icmp-object *icmp_type*

Syntax Description

icmp_type	Specifies an ICMP type name or number (0-255).

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Icmp-type configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **icmp-object** command is used with the **object-group icmp-type** command to define an ICMP object. It is used in icmp-type configuration mode.

Instead of using this command, use **object-group service** and **service-group** commands to create a service group that contains ICMP types. Service groups can include ICMP6 and ICMP codes, whereas ICMP objects cannot.

ICMP type numbers and names include:

Number	ICMP Type Name
0	**echo-reply**
3	**unreachable**
4	**source-quench**
5	**redirect**
6	**alternate-address**
8	**echo**

Number	ICMP Type Name
9	**router-advertisement**
10	**router-solicitation**
11	**time-exceeded**
12	**parameter-problem**
13	**timestamp-request**
14	**timestamp-reply**
15	**information-request**
16	**information-reply**
17	**address-mask-request**
18	**address-mask-reply**
31	**conversion-error**
32	**mobile-redirect**

Examples

The following example shows how to use the **icmp-object** command in icmp-type configuration mode:

```
ciscoasa(config)# object-group icmp-type icmp_allowed
ciscoasa(config-icmp-type)# icmp-object echo
ciscoasa(config-icmp-type)# icmp-object time-exceeded
ciscoasa(config-icmp-type)# exit
```

Related Commands

Command	Description
clear configure object-group	Removes all the **object-group** commands from the configuration.
object-group	Defines object groups to optimize your configuration.
show running-config object-group	Displays the current object groups.

icmp unreachable

To configure the unreachable ICMP message rate limit for ICMP traffic that terminates at an ASA interface, use the **icmp unreachable** command. To remove the configuration, use the **no** form of this command.

icmp unreachable rate-limit *rate* **burst-size** *size*
no icmp unreachable rate-limit *rate* **burst-size** *size*

Syntax Description

rate-limit *rate*	Sets the rate limit of unreachable messages, between 1 and 100 messages per second. The default is 1 message per second.
burst-size *size*	Sets the burst rate, between 1 and 10. The burst size number of reponses are sent, but subsequent replies are not sent until the rate limit is reached.

Command Default

The default rate limit is 1 message per second.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(2)	This command was added.

Usage Guidelines

If you allow ICMP messages, including unreachable messages, to be sent to an ASA interface (see the **icmp** command), then you can control the rate of unreachable messages.

This command, along with the **set connection decrement-ttl** command, is required to allow a traceroute through the ASA that shows the ASA as one of the hops.

Examples

The following example enables time to live decrements and sets the ICMP unreachable rate limit:

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class local_server
ciscoasa(config-pmap-c)# set connection decrement-ttl
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# icmp permit host 172.16.2.15 echo-reply outside
ciscoasa(config)# icmp permit 172.22.1.0 255.255.0.0 echo-reply outside
ciscoasa(config)# icmp permit any unreachable outside
ciscoasa(config)# icmp unreachable rate-limit 50 burst-size 10
```

Related Commands

Commands	Description
clear configure icmp	Clears the ICMP configuration.
debug icmp	Enables the display of debug information for ICMP.
set connection decrement-ttl	Decrements the time to live value for a packet.
show icmp	Displays ICMP configuration.
timeout icmp	Configures the idle timeout for ICMP.

id-cert-issuer

To indicate whether the system accepts peer certificates issued by the CA associated with this trustpoint, use the **id-cert-issuer** command in crypto ca-trustpoint configuration mode. To disallow certificates that were issued by the CA associated with the trustpoint, use the **no** form of this command. This is useful for trustpoints that represent widely used root CAs.

id-cert-issuer
no id-cert-issuer

Syntax Description

This command has no arguments or keywords.

Command Default

The default setting is enabled (identity certificates are accepted).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca-trustpoint configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use this command to limit certificate acceptance to those issued by the subordinate certificate of a widely used root certificate. If you do not allow this feature, the ASA rejects any IKE peer certificate signed by this issuer.

Examples

The following example enters crypto ca trustpoint configuration mode for the trustpoint central, and lets an administrator accept identity certificates signed by the issuer for the trustpoint central:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# id-cert-issuer
ciscoasa(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.
enrollment retry count	Specifies the number of retries to attempt to send an enrollment request.

Command	Description
enrollment retry period	Specifies the number of minutes to wait before trying to send an enrollment request.
enrollment terminal	Specifies cut-and-paste enrollment with this trustpoint.

id-mismatch

To enable logging for excessive DNS ID mismatches, use the **id-mismatch** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

id-mismatch [**count** *number* **duration** *seconds*] **action log**
id-mismatch [**count** *number* **duration** *seconds*] **action log**]

Syntax Description

count number	The maximum number of mismatch instances before a system message log is sent.
duration seconds	The period, in seconds, to monitor.

Command Default

This command is disabled by default. The default rate is 30 in the a period of 3 seconds if the options are not specified when the command is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

A high rate of DNS ID mismatches may indicate a cache poisoning attack. This command can be enabled to monitor and alert such attempts. A summarized system message log will be printed if the mismatch rate exceeds the configured value. The **id-mismatch** command provides the system administrator with additional information to the regular event-based system message log.

Examples

The following example shows how to enable ID mismatch in a DNS inspection policy map:

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# id-mismatch action log
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.

Command	Description
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

id-randomization

To randomize the DNS identifier for a DNS query, use the **id-randomization** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

id-randomization
no id-randomization

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled by default. The DNS identifier from the DNS query does not get modified.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

ID randomization helps protect against cache poisening attacks.

Examples

The following example shows how to enable ID randomization in a DNS inspection policy map:

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# id-randomization
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

id-usage

To specify how the enrolled identity of a certificate can be used, use the **id-usage** command in crypto ca trustpoint configuration mode. To set the usage of the certificate to the default, use the **no** form of this command.

id-usage { **ssl-ipsec** | **code-signer** }
no id-usage { **ssl-ipsec code-signer** }

Syntax Description

code-signer	The device identity represented by this certificate is used as a Java code signer to verify applets provided to remote users.
ssl-ipsec	(Default) The device identity represented by this certificate can be used as the server-side identity for SSL or IPsec-encrypted connections.

Command Default

The **id-usage** command default is **ssl-ipsec**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca trustpoint configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Remote-access VPNs can use SSL, IPsec, or both protocols, depending on deployment requirements, to permit access to virtually any network application or resource. The **id-usage** command allows you to specify the type of access to various certificate-protected resources.

A CA identity and in some cases, a device identity, is based on a certificate issued by the CA. All of the commands within the crypto ca trustpoint configuration mode control CA-specific configuration parameters, which specify how the ASA obtains the CA certificate, how the ASA obtains its certificate from the CA, and the authentication policies for user certificates issued by the CA.

Only a single instance of the **id-usage** command can be present in a trustpoint configuration. To enable the trustpoint for the **code-signer** and/or **ssl-ipsec** options, use a single instance which can specify either or both options.

Examples

The following example enters crypto ca trustpoint configuration mode for the trustpoint central, and designates it as a code-signer certificate:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)# id-usage code-signer
ciscoasa(config-ca-trustpoint)#
```

The following example enters crypto ca trustpoint configuration mode for the trustpoint general, and designates it as both a code-signer certificate and as a server side identity for SSL or IPsec connections:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)# id-usage code-signer ssl-ipsec
ciscoasa(config-ca-trustpoint)#
```

The following example enters crypto ca trustpoint configuration mode for the trustpoint checkin1, and resets it to limit its use to SSL or IPsec connections:

```
ciscoasa(config)# crypto ca trustpoint checkin1
ciscoasa(config-ca-trustpoint)# no
 id-usage ssl-ipsec
ciscoasa(config-ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca trustpoint configuration mode.
java-trustpoint	Configures the WebVPN Java object signing facility to use a PKCS12 certificate and keying material from a specified trustpoint location.
ssl trust-point	Specifies the certificate that represents the SSL certificate for an interface.
trust-point (tunnel-group ipsec-attributes mode)	Specifies the name that identifies the certificate to be sent to the IKE peer,
validation-policy	Specifies conditions for validating certificates associated with user connections.

igmp

To reinstate IGMP processing on an interface, use the **igmp** command in interface configuration mode. To disable IGMP processing on an interface, use the **no** form of this command.

igmp
no igmp

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Only the **no** form of this command appears in the running configuration.

Examples

The following example disables IGMP processing on the selected interface:

```
ciscoasa(config-if)# no igmp
```

Related Commands

Command	Description
show igmp groups	Displays the multicast groups with receivers that are directly connected to the ASA and that were learned through IGMP.
show igmp interface	Displays multicast information for an interface.

igmp access-group

To control the multicast groups that hosts on the subnet serviced by an interface can join, use the **igmp access-group** command in interface configuration mode. To disable groups on the interface, use the **no** form of this command.

igmp access-group *acl*
no igmp access-group *acl*

Syntax Description

acl	Name of an IP access list. You can specify a standard or and extended access list. However, if you specify an extended access list, only the destination address is matched; you should specify **any** for the source.

Command Default

All groups are allowed to join on an interface.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Examples

The following example limits hosts permitted by access list 1 to join the group:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp access-group 1
```

Related Commands

Command	Description
show igmp interface	Displays multicast information for an interface.

igmp forward interface

To enable forwarding of all IGMP host reports and leave messages received to the interface specified, use the **igmp forward interface** command in interface configuration mode. To remove the forwarding, use the **no** form of this command.

igmp forward interface *if-name*
no igmp forward interface *if-name*

Syntax Description

if-name	Logical name of the interface.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Usage Guidelines

Enter this command on the input interface. This command is used for stub multicast routing and cannot be configured concurrently with PIM.

Examples

The following example forwards IGMP host reports from the current interface to the specified interface:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp forward interface outside
```

Related Commands

Command	Description
show igmp interface	Displays multicast information for an interface.

igmp join-group

To configure an interface to be a locally connected member of the specified group, use the **igmp join-group** command in interface configuration mode. To cancel membership in the group, use the **no** form of this command.

igmp join-group *group-address*
no igmp join-group *group-address*

Syntax Description

group-address	IP address of the multicast group.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Usage Guidelines

This command configures an ASA interface to be a member of a multicast group. The **igmp join-group** command causes the ASA to both accept and forward multicast packets destined for the specified multicast group.

To configure the ASA to forward the multicast traffic without being a member of the multicast group, use the **igmp static-group** command.

Examples

The following example configures the selected interface to join the IGMP group 255.2.2.2:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp join-group 225.2.2.2
```

Related Commands

Command	Description
igmp static-group	Configure the interface to be a statically connected member of the specified multicast group.

igmp limit

To limit the number of IGMP states on a per-interface basis, use the **igmp limit** command in interface configuration mode. To restore the default limit, use the **no** form of this command.

igmp limit *number*
no igmp limit [*number*]

Syntax Description

number	Number of IGMP states allowed on the interface. Valid values range from 0 to 5000. The default value is 500. Setting this value to 0 prevents learned groups from being added, but manually defined memberships (using the **igmp join-group** and **igmp static-group** commands) are still permitted.

Command Default

The default is 500.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added. It replaced the **igmp max-groups** command.
9.15(1) *Also in 9.12(4)*	The igmp limit was increased from 500 to 5000.

Usage Guidelines

This command configures the limit of IGMP states. Membership reports exceeding the configured limits are not entered in the IGMP cache, and traffic for the excess membership reports is not forwarded.

When you change the IGMP limit on the interface with active joins on it, the new limit is not applicable to the existing groups. ASA validates the limit only when a new group is added to the interface or when the IGMP join timers expire. To apply the new limit with immediate effect, you must disenable and re-enable IGMP on the interface.

Examples

The following example limits the number of IGMP states on the interface to 250:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp limit 250
```

Related Commands

Command	Description
igmp	Reinstates IGMP processing on an interface.
igmp join-group	Configure an interface to be a locally connected member of the specified group.
igmp static-group	Configure the interface to be a statically connected member of the specified multicast group.

igmp query-interval

To configure the frequency at which IGMP host query messages are sent by the interface, use the **igmp query-interval** command in interface configuration mode. To restore the default frequency, use the **no** form of this command.

igmp query-interval *seconds*
no igmp query-interval *seconds*

Syntax Description

seconds	Frequency, in seconds, at which to send IGMP host query messages. Valid values range from 1 to 3600. The default is 125 seconds.

Command Default

The default query interval is 125 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Usage Guidelines

Multicast routers send host query messages to discover which multicast groups have members on the networks attached to the interface. Hosts respond with IGMP report messages indicating that they want to receive multicast packets for specific groups. Host query messages are addressed to the all-hosts multicast group, which has an address of 224.0.0.1 TTL value of 1.

The designated router for a LAN is the only router that sends IGMP host query messages:

- For IGMP Version 1, the designated router is elected according to the multicast routing protocol that runs on the LAN.
- For IGMP Version 2, the designated router is the lowest IP-addressed multicast router on the subnet.

If the router hears no queries for the timeout period (controlled by the **igmp query-timeout** command), it becomes the querier.

Caution Changing this value may severely impact multicast forwarding.

Examples

The following example changes the IGMP query interval to 120 seconds:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp query-interval 120
```

Related Commands

Command	Description
igmp query-max-response-time	Configures the maximum response time advertised in IGMP queries.
igmp query-timeout	Configures the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying.

igmp query-max-response-time

To specify the maximum response time advertised in IGMP queries, use the **igmp query-max-response-time** command in interface configuration mode. To restore the default response time value, use the **no** form of this command.

igmpquery-max-response-time*seconds*
no igmp query-max-response-time *seconds*

Syntax Description

seconds	Maximum response time, in seconds, advertised in IGMP queries. Valid values are from 1 to 25. The default value is 10 seconds.

Command Default

10 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Usage Guidelines

This command is valid only when IGMP Version 2 or 3 is running.

This command controls the period during which the responder can respond to an IGMP query message before the router deletes the group.

Examples

The following example changes the maximum query response time to 8 seconds:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp query-max-response-time 8
```

Related Commands

Command	Description
igmp query-interval	Configures the frequency at which IGMP host query messages are sent by the interface.
igmp query-timeout	Configures the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying.

igmp query-timeout

To configure the timeout period before the interface takes over as the querier after the previous querier has stopped querying, use the **igmp query-timeout** command in interface configuration mode. To restore the default value, use the **no** form of this command.

igmpquery-timeout*seconds*
no igmp query-timeout *seconds*

Syntax Description

seconds	Number of seconds that the router waits after the previous querier has stopped querying and before it takes over as the querier. Valid values are from 60 to 300 seconds. The default value is 255 seconds.

Command Default

The default query interval is 255 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command requires IGMP Version 2 or 3.

Examples

The following example configures the router to wait 200 seconds from the time it received the last query before it takes over as the querier for the interface:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp query-timeout 200
```

Related Commands

Command	Description
igmp query-interval	Configures the frequency at which IGMP host query messages are sent by the interface.
igmp query-max-response-time	Configures the maximum response time advertised in IGMP queries.

igmp static-group

To configure the interface to be a statically connected member of the specified multicast group, use the **igmp static-group** command in interface configuration mode. To remove the static group entry, use the **no** form of this command.

igmp static-group *group*
no igmp static-group *group*

Syntax Description

group	IP multicast group address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

When configured with the **igmp static-group** command, the ASA interface does not accept multicast packets destined for the specified group itself; it only forwards them. To configure the ASA to both accept and forward multicast packets for a specific multicast group, use the **igmp join-group** command. If the **igmp join-group** command is configured for the same group address as the **igmp static-group** command, the **igmp join-group** command takes precedence, and the group behaves like a locally joined group.

Examples

The following example adds the selected interface to the multicast group 239.100.100.101:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp static-group 239.100.100.101
```

Related Commands

Command	Description
igmp join-group	Configures an interface to be a locally connected member of the specified group.

igmp version

To configure which version of IGMP the interface uses, use the **igmp version** command in interface configuration mode. To restore version to the default, use the **no** form of this command.

igmp version { **1** | **2** }
no igmp version [**1** | **2**]

Syntax Description

1	IGMP Version 1.
2	IGMP Version 2.

Command Default

IGMP Version 2.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Usage Guidelines

All routers on the subnet must support the same version of IGMP. Hosts can have any IGMP version (1 or 2), and the ASA will correctly detect their presence and query them appropriately.

Some commands require IGMP Version 2, including as the **igmp query-max-response-time** and **igmp query-timeout** commands.

Examples

The following example configures the selected interface to use IGMP Version 1:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp version 1
```

Related Commands

Command	Description
igmp query-max-response-time	Configures the maximum response time advertised in IGMP queries.

Command	Description
igmp query-timeout	Configures the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying.

ignore-ipsec-keyusage (Deprecated)

To suppress key usage checking on IPsec client certificates, use the **ignore-ipsec-keyusage** command in ca-trustpoint configuration mode. To resume key usage checking, use the **no** form of this command.

ignore-ipsec-keyusage
no ignore-ipsec-keyusage

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca-trustpoint configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added as a safety measure and was deprecated at the same time. Note that future releases might not offer suppression of key usage checking.

Usage Guidelines

Use of this command indicates that the values in the Key Usage and extended Key Usage extensions of IPsec remote client certificates are not to be validated. This command ignores key usage checking and is useful for non-compliant deployments.

Examples

The following example shows how to ignore the results of key usage checking:

```
ciscoasa(config)#
crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)#
ciscoasa(config-ca-trustpoint)# ignore-ipsec-keyusage
Notice: This command has been deprecated
ciscoasa(config-ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca trustpoint configuration mode.

ignore lsa mospf

To suppress the sending of syslog messages when the router receives LSA Type 6 MOSPF packets, use the **ignore lsa mospf** command in router configuration mode. To restore the sending of the syslog messages, use the **no** form of this command.

ignore lsa mospf
no ignore lsa mospf

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Type 6 MOSPF packets are unsupported.

Examples

The following example causes LSA Type 6 MOSPF packets to be ignored:

```
ciscoasa(config-router)# ignore lsa mospf
```

Related Commands

Command	Description
show running-config router ospf	Displays the OSPF router configuration.

ignore-lsp-errors

To allow the ASA to ignore IS-IS link-state packets that are received with internal checksum errors rather than purging the link-state packets, use the **ignore-lsp-errors** command in router isis configuration mode. To disable this function, use the **no** form of this command.

ignore-lsp-errors
no ignore-lsp-errors

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default, that is, corrupted LSPs are dropped instead of purged for network stability.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router isis configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

The IS-IS protocol definition requires that a received link-state packet with an incorrect data-link checksum be purged by the receiver, which causes the initiator of the packet to regenerate it. However, if a network has a link that causes data corruption while still delivering link-state packets with correct data link checksums, a continuous cycle of purging and regenerating large numbers of packets can occur.

Because this could render the network nonfunctional, use the **ignore-lsp-errors** command to ignore these link-state packets rather than purge the packets. Link-state packets are used by the receiving routers to maintain their routing tables.

If you want to explicitly purge the corrupted LSPs, issue the **no ignore-lsp-errors** command.

Examples

The following example instructs the router to ignore link-state packets that have internal checksum errors:

ciscoasa(config)# **router isis**

```
ciscoasa(config-router)# ignore-lsp-errors
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.

Command	Description
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.

Command	Description
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

ignore-ssl-keyusage (Deprecated)

To suppress key usage checking on SSL client certificates, use the **ignore-ssl-keyusage** command in ca-trustpoint configuration mode. To resume key usage checking, use the **no** form of this command.

ignore-ssl-keyusage
no ignore-ssl-keyusage

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca-trustpoint configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added as a safety measure and was deprecated at the same time. Note that future releases might not offer suppression of key usage checking.

Usage Guidelines

Use of this command indicates that the values in the Key Usage and extended Key Usage extensions of IPsec remote client certificates are not to be validated. This command ignores key usage checking and is useful for noncompliant deployments.

Examples

The following example shows how to ignore the results of key usage checking:

```
ciscoasa(config)#
crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)#
ciscoasa(config-ca-trustpoint)# ignore-ssl-keyusage
Notice: This command has been deprecated
ciscoasa(config-ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca trustpoint configuration mode.

ike-retry-count

To configure the maximum number of connection retry attempts a Cisco AnyConnect VPN Client using IKE should make before falling back to SSL to attempt the connection, use the **ike-retry-count** command in group-policy webvpn configuration mode or username webvpn configuration mode. To remove this command from the configuration and reset the maximum number of retry attempts to the default value, use the **no** form of this command.

ike-retry-count { **none** | *value* }
no ike-retry-count { **none** | *value* }

Syntax Description

none	Specifies that no retry attempts are allowed.
value	Specify the maximum number of connection retry atttempts (1-10) for the Cisco AnyConnect VPN Client to perform after an initial connection failure.

Command Default

The default number of allowed retry attempts is 3.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy webvpn configuration	• Yes	—	• Yes	—	—
Username webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added

Usage Guidelines

Use the **ike-retry-count** command to control the number of times that the Cisco AnyConnect VPN Client should attempt to connect using IKE. If the client fails to connect using IKE after the number of retries specified in this command, it falls back to SSL to attempt the connection. This value overrides any value that exists in the Cisco AnyConnect VPN Client.

Note To support fallback from IPsec to SSL, the **vpn-tunnel-protocol** command must be have with both the **svc** and **ipsec** arguments configured.

Examples

The following example sets the IKE retry count to 7 for the group policy named FirstGroup:

```
ciscoasa
(config)# group-policy FirstGroup attributes
ciscoasa
(config-group-policy)# webvpn
ciscoasa
(config-group-webvpn)# ike-retry-count 7
ciscoasa
(config-group-webvpn)#
```

The following example sets the IKE retry count to 9 for the username Finance:

```
ciscoasa
(config)#
username
Finance attributes
ciscoasa
(config-username)# webvpn
ciscoasa
(config-username-webvpn)# ike-retry-count 9
ciscoasa
(config-group-webvpn)#
```

Related Commands

Command	Description
group-policy	Creates or edits a group policy.
ike-retry-timeout	Specifies the number of seconds between IKE retry attempts.
username	Adds a user to the ASA database.
vpn-tunnel-protocol	Configures a VPN tunnel type (IPsec, L2TP over IPsec, or WebVPN).
webvpn	Enters group-policy webvpn configuration mode or username webvpn configuration mode.

ikev1 pre-shared-key

To specify a preshared key to support IKEv1 connections based on preshared keys, use the **pre-shared-key** command in tunnel-group ipsec-attributes configuration mode. To return to the default value, use the **no** form of this command.

pre-shared-key*key*
no pre-shared-key

Syntax Description

key	Specifies an alphanumeric key between 1 and 128 characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ipsec-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
8.4(1)	The command name was changed from pre-shared-key to ikev1 pre-shared-key.

Usage Guidelines

You can apply this attribute to all IPsec tunnel-group types.

Examples

The following command entered in config-ipsec configuration mode, specifies the preshared key XYZX to support IKE connections for the IPSec LAN-to-LAN tunnel group named 209.165.200.225:

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# pre-shared-key xyzx
ciscoasa(config-tunnel-ipsec)#
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.

Command	Description
tunnel-group ipsec-attributes	Configures the tunnel group IPsec attributes for this group.

ikev1 trust-point

To specify the name of a trustpoint that identifies the certificate to be sent to the IKEv1 peer, use the **trust-point** command in tunnel-group ipsec-attributes mode. To eliminate a trustpoint specification, use the **no** form of this command.

trust-point*trust-point-name*
no trust-point *trust-point-name*

Syntax Description

trust-point-name	Specifies the name of the trustpoint to use.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ipsec attributes	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
8.4(1)	The command name was changed from trust-point to ikev1 trust-point.

Usage Guidelines

You can apply this attribute to all IPsec tunnel group types.

Examples

The following example entered in tunnel-ipsec configuration mode, configures a trustpoint for identifying the certificate to be sent to the IKEv1 peer for the IPsec LAN-to-LAN tunnel group named 209.165.200.225:

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev1 trust-point mytrustpoint
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.

Command	Description
tunnel-group ipsec-attributes	Configures the tunnel group IPsec attributes for this group.

ikev1 user-authentication

To configure hybrid authentication during IKE, use the **ikev1 user-authentication** command in tunnel-group ipsec-attributes configuration mode. To disable hybrid authentication, use the **no** form of this command.

ikev1 user-authentication [*interface*] { **none** | **xauth** | **hybrid** }
no ikev1 user-authentication [*interface*] { **none** | **xauth** | **hybrid** }

Syntax Description

hybrid	Specifies hybrid XAUTH authentication during IKE.
interface	(Optional) Specifies the interface on which the user authentication method is configured.
none	Disables user authentication during IKE.
xauth	Specifies XAUTH, also called extended user authentication.

Command Default

The default authentication method is XAUTH or extended user authentication. The default is all interfaces.

Note You must leave the value at the XAUTH default to avoid breaking any established L2TP over IPsec sessions. If the tunnel-group is set to any other value (such as isakmp ikev1-user-authentication none), then you cannot establish an L2TP over IPsec session.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ipsec-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
8.4(1)	The command name was changed from isakmp **ikev1-user-authentication** to **ikev1 user-authentication.**

Usage Guidelines

You use this command when you need to use digital certificates for ASA authentication and a different, legacy method for remote VPN user authentication, such as RADIUS, TACACS+, or SecurID. This command breaks Phase 1 of IKE down into the following two steps, together called hybrid authentication:

1. The ASA authenticates to the remote VPN user with standard public key techniques. This establishes an IKE security association that is unidirectionally authenticated.
2. An XAUTH exchange then authenticates the remote VPN user. This extended authentication can use one of the supported legacy authentication methods.

Note Before the authentication type can be set to hybrid, you must configure the authentication server, create a preshared key, and configure a trustpoint.

An IPsec hybrid RSA authentication type is rejected when the exchange type is main mode.

When you omit the optional *interface* argument, the command applies to all the interfaces and serves as a backup when the per-interface command is not specified. When there are two **ikev1 user-authentication** commands specified for a tunnel group, and one uses the *interface* argument and one does not, the one specifying the interface takes precedence for that particular interface.

Examples

The following example commands enable hybrid XAUTH on the inside interface for a tunnel group called example-group:

```
ciscoasa(config)# tunnel-group example-group type ipsec-ra
ciscoasa(config)# tunnel-group example-group ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev1 user-authentication (inside) hybrid
ciscoasa(config-tunnel-ipsec)#
```

Related Commands

Command	Description
aaa-server	Defines a AAA server.
pre-shared-key	Creates a preshared key for supporting IKE connections.
tunnel-group	Creates and manages the database of connection specific records for IPsec, L2TP/IPsec, and WebVPN connections.

ikev2 local-authentication

To specify local authentication for IKEv2 LAN-to-LAN connections, use the **ikev2 local-authentication** command in tunnel-group ipsec-attributes configuration mode. To return to the default value, use the **no** form of this command.

ikev2 local-authentication { **pre-shared-key** *key_value* | **hex** < *string* > | **certificate trustpoint**
no ikev2 local-authentication { **pre-shared-key** *key_value* | **hex** < *string* > | **certificate trustpoint**

Syntax Description

certificate	Specifies certificate authentication.
hex	Configures a hex pre-shared key.
key_value	The key value, from 1 to 128 characters.
pre-shared-key	Specifies a local preshared key that is used to authenticate the remote peer.
string	Enter a hex pre-shared key between 2 and 256 with an even number of characters.
trustpoint	Specifies the trustpoint that identifies the certificate to send to the remote peer.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ipsec-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(1)	This command was added.
9.3(2)	Remote authentication using EAP was added.
9.4(1)	The hex and hex string keywords were added.

Usage Guidelines

This command applies to IPsec IKEv2 LAN-to-LAN tunnel groups only.

You may configure only one authentication option for local authentication.

You must configure this command using the **certificate** option before you may use the **ikev2 remote-authentication** command to enable EAP authentication.

For IKEv2 connections, the tunnel group mapping must know which authentication methods to allow for remote authentication (PSK, certificate, and EAP) and local authentication (PSK and certificate), and which trust point to use for local authentication.

Examples

The following command specifies the preshared key XYZX to support IKE connections for the IPsec LAN-to-LAN tunnel group named 209.165.200.225:

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_l2l
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key XYZX
```

The following commands configure the remote access tunnel group to authenticate the ASA to the peer using its identity certificate, which is associated with the trustpoint, myIDcert. The peer may also be authenticated using a preshared key, certificate, or EAP.

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_l2l
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication pre-shared-key XYZX
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication certificate
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication eap query-identity
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication certificate myIDcert
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group ipsec-attributes	Configures the tunnel group IPsec attributes for this group.

ikev2 mobike-rrc

To enable return routability checking during mobile IKE (mobike) communications for IPsec IKEv2 RA VPN connections, use the **ikev2 mobike-rrc** command in tunnel-group ipsec-attributes configuration mode. To disable return routability checking, use the **no** form of this command.

ikev2 mobike-rrc
no ikev2 mobike-rrc

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Mobike is “always on.” This command is used to enable RRC for mobike connections.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ipsec-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.8(1)	This command was added.

Usage Guidelines

This command applies to IPsec IKEv2 RA VPN tunnel groups only.

Examples

The following example commands enable the return routability check for mobike for a tunnel group called example-group:

```
ciscoasa(config)# tunnel-group example-group type ipsec-ra
ciscoasa(config)# tunnel-group example-group ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev2 mobike-rrc
ciscoasa(config-tunnel-ipsec)#
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.

Command	Description
tunnel-group ipsec-attributes	Configures the tunnel group IPsec attributes for this group.

ikev2 remote-authentication

To specify remote authentication for IPsec IKEv2 LAN-to-LAN connections, use the **ikev2 remote-authentication** command in tunnel-group ipsec-attributes configuration mode. To return to the default value, use the **no** form of this command.

ikev2 remote-authentication { **pre-shared-key** *key_value* | **certificate** | **hex <string>** | **eap** [**query-identity**] }
no ikev2 remote-authentication { **pre-shared-key** *key_value* | **certificate** | **hex <string>** | **eap** [**query-identity**] }

Syntax Description

certificate	Specifies certificate authentication.
eap	Specifies the Extensible Authentication Protocol (EAP) is the method that supports user authentication with generic, third-party IKEv2 remote access clients (in addition to AnyConnect).
hex	Configure a hex pre-shared key.
key_value	The key value, from 1 to 128 characters.
pre-shared-key	Specifies a local preshared key that is used to authenticate the remote peer.
query-identity	Requests the EAP identity from the peer.
string	Enter a hex pre-shared key between 2 and 256 with an even number of characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ipsec-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(1)	This command was added.
9.3(2)	The **eap** and **query-identity** keywords were added.
9.4(1)	The hex and hex-string keywords were added.

Usage Guidelines

This command applies to IPsec IKEv2 LAN-to-LAN tunnel groups only.

Before you can enable EAP for remote authentication, you must configure local authentication using a certificate and a valid trustpoint using the **ikev2 local-authentication pre-shared-key** *key-value* | **certificate** *trustpoint* command. Otherwise, an error occurs and the EAP authentication request is rejected.

You may configure multiple authentication options for remote authentication.

Note For IKEv2 connections, the tunnel group mapping must know which authentication methods to allow for remote authentication (PSK, certificate, and EAP) and local authentication (PSK and certificate), and which trust point to use for local authentication. Currently, mapping is performed using the IKE ID, which is taken from the peer or peer certificate field value (using the certificate map). If both options fail, then the in-coming connection is mapped to the default remote access tunnel group. A certificate map is an applicable option only when the remote peer is authenticated via a certificate. This map allows mapping to different tunnel groups. For certificate authentication only, the tunnel group lookup is performed using rules or using the default setting. For EAP and PSK authentication, the tunnel group lookup is performed using the IKE ID on the client (it matches the tunnel group name) or using the default setting.

Examples

The following commands specify the preshared key XYZX to support IKEv2 connections for the IPsec LAN-to-LAN tunnel group named 209.165.200.225:

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication pre-shared-key xyzx
```

The following commands show an EAP request for authentication being denied:

```
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication eap query-identity
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication certificate
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key 12345678
ERROR: The local-authentication method is required to be certificate based
if remote-authentication allows EAP
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication certificate myIDcert
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group ipsec-attributes	Configures the tunnel group IPsec attributes for this group.

ikev2 rsa-sig-hash

To configure the IKEv2 RSA signature hash, use the **ikev2 rsa-sig-hash** command in tunnel-group ipsec-attributes configuration mode. To return to the default value, use the **no** form of this command.

ikev2rsa-sig-hashsha1
no ikev2 rsa-sig-hash sha1

Syntax Description

sha1	Signs the IKEv2 authentication payload with the SHA-1 hash function.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ipsec-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.12(1)	This command was added.

Usage Guidelines

This command applies to IPsec IKEv2 LAN-to-LAN tunnel groups only.

Examples

The following commands sign the IKEv2 authentication payload with the SHA-1 function:

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev2 rsa-sig-hash sha
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group ipsec-attributes	Configures the tunnel group IPsec attributes for this group.

im

To enable instant messaging over SIP, use the **im** command in parameters configuration mode, which is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

im
noim

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to enable instant messaging over SIP in a SIP inspection policy map:

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# im
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

imap4s (Deprecated)

Note The last supported release for this command was 9.5(1).

To enter IMAP4S configuration mode, use the **imap4s** command in global configuration mode. To remove any commands entered in IMAP4S command mode, use the **no** form of this command.

imap4s
no imap4s

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.5(2)	This command was deprecated.

Usage Guidelines

IMAP4 is a client/server protocol in which your Internet server receives and holds e-mail for you. You (or your e-mail client) can view just the heading and the sender of the letter and then decide whether to download the mail. You can also create and manipulate multiple folders or mailboxes on the server, delete messages, or search for certain parts or an entire note. IMAP requires continual access to the server during the time that you are working with your mail. IMAP4S lets you receive e-mail over an SSL connection.

Examples

The following example shows how to enter IMAP4S configuration mode:

```
ciscoasa
(config)#
 imap4s
ciscoasa(config-imap4s)#
```

Related Commands

Command	Description
clear configure imap4s	Removes the IMAP4S configuration.
show running-config imap4s	Displays the running configuration for IMAP4S.

imi-traffic-descriptor

To define an action when the IMI Traffic Descriptor (IMITD) option occurs in a packet header with IP Options inspection, use the **imi-traffic-descriptor** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

imi-traffic-descriptor action { **allow** | **clear** }
no imi-traffic-descriptor action { **allow** | **clear** }

Syntax Description

allow	Allow packets containing the IMI Traffic Descriptor IP option.
clear	Remove the IMI Traffic Descriptor option from packet headers and then allow the packets.

Command Default

By default, IP Options inspection drops packets containing the IMI Traffic Descriptor IP option.

You can change the default using the **default** command in the IP Options inspection policy map.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(1)	This command was added.

Usage Guidelines

This command can be configured in an IP Options inspection policy map.

You can configure IP Options inspection to control which IP packets with specific IP options are allowed through the ASA. You can allow a packet to pass without change or clear the specified IP options and then allow the packet to pass.

Examples

The following example shows how to set up an action for IP Options inspection in a policy map:

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# imi-traffic-descriptor action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.

Command	Description
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

import

To provide one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface to StateLess Address Auto Configuration (SLAAC) clients, use the **import** command in ipv6 dhcp pool configuration mode. To remove the parameters, use the **no** form of this command.

import { [**dns-server**] [**domain-name**] [**nis address**] [**nis domain-name**] [**nisp address**] [**nisp domain-name**] [**sip address**] [**sip domain-name**] [**sntp address**] }
no import { [**dns-server**] [**domain-name**] [**nis address**] [**nis domain-name**] [**nisp address**] [**nisp domain-name**] [**sip address**] [**sip domain-name**] [**sntp address**] }

Syntax Description

dns-server	Imports the domain name server (DNS) server IP address.
domain-name	Imports the domain name.
nis address	Imports the Network Information Service (NIS) server IP address.
nis domain-name	Imports the NIS domain name.
nisp address	Imports the Network Information Service Plus (NIS+) server IP address.
nisp domain-name	Imports the NIS+ domain name.
sip address	Imports the Session Initiation Protocol (SIP) server IP address.
sip domain-name	Imports the SIP domain name.
sntp address	Imports the Simple Network Time Protocol (SNTP) server IP address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ipv6 dhcp pool configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

For clients that use SLAAC in conjunction with the Prefix Delegation feature, you can configure the ASA to provide information in an **ipv6 dhcp pool**, including the DNS server or domain name, when they send

Information Request (IR) packets to the ASA. You can mix and match manually-configured parameters with imported parameters; however, you cannot configure the same parameter manually and in the **import** command. The ASA only accepts IR packets, and does not assign addresses to the clients. Configure the DHCPv6 stateless server using the **ipv6 dhcp server** command; you specify an **ipv6 dhcp pool** name when you enable the server.

Configure Prefix Delegation using the **ipv6 dhcp client pd** command.

This feature is not supported in clustering.

Examples

The following example creates two IPv6 DHCP pools, and enables the DHCPv6 server on two interfaces:

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
import dns-server
ipv6 dhcp pool IT-Pool
domain-name it.example.com
import dns-server
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

Related Commands

Command	Description
clear ipv6 dhcp statistics	Clears DHCPv6 statistics.
domain-name	Configures the domain name provided to SLAAC clients in responses to IR messages.
dns-server	Configures the DNS server provided to SLAAC clients in responses to IR messages.
import	Uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface, and provides them to SLAAC clients in responses to IR messages.
ipv6 address	Enables IPv6 and configures the IPv6 addresses on an interface.
ipv6 address dhcp	Obtains an address using DHCPv6 for an interface.
ipv6 dhcp client pd	Uses a delegated prefix to set the address for an interface.
ipv6 dhcp client pd hint	Provides one or more hints about the delegated prefix you want to receive.
ipv6 dhcp pool	Creates a pool that includes information that you want to provide to SLAAC clients on a given interface using the DHCPv6 stateless server.

Command	Description
ipv6 dhcp server	Enables the DHCPv6 stateless server.
network	Configures BGP to advertise the delegated prefix received from the server.
nis address	Configures the NIS address provided to SLAAC clients in responses to IR messages.
nis domain-name	Configures the NIS domain name provided to SLAAC clients in responses to IR messages.
nisp address	Configures the NISP address provided to SLAAC clients in responses to IR messages.
nisp domain-name	Configures the NISP domain name provided to SLAAC clients in responses to IR messages.
show bgp ipv6 unicast	Displays entries in the IPv6 BGP routing table.
show ipv6 dhcp	Shows DHCPv6 information.
show ipv6 general-prefix	Shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes.
sip address	Configures the SIP address provided to SLAAC clients in responses to IR messages.
sip domain-name	Configures the SIP domain name provided to SLAAC clients in responses to IR messages.
sntp address	Configures the SNTP address provided to SLAAC clients in responses to IR messages.

import webvpn AnyConnect-customization

To load an AnyConnect customization object onto the flash device of the ASA, enter the **import webvpn AnyConnect-customization** command in privileged EXEC mode.

import webvpn AnyConnect-customization type { **binary** | **resource** | **transform** } **platform** { **linux** | **linux-64** | **mac-intel** | **mac-powerpc** | **win** | **win-mobile** } **name** *name* { *URL* | **stdin** { *num_chars* | *data* **quit** } }

Syntax Description

name	The name that identifies the customization object. The maximum number is 64 characters.
platform {**linux** | **linux-64** | **mac-intel** | **mac-powerpc** | **win** | **win-mobile**}	Client platform to which the object applies.
stdin {*num_chars data* | *data* **quit**}	Specifies that the data will be provided from stdin. If the number of characters is not specified then the data read from standard input is expected to be base64-encoded followed by "\nquit\n".
type {**binary** | **resource** | **transform**}	Type of customization object being imported.
URL	Remote path to the source of the XML customization object. The maximum number is 255 characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Make sure WebVPN is enabled on an ASA interface before you enter the **import customization** command. To do so, enter the **show running-config** command.

The ASA copies the customization object from the URLor stdin to the ASA file system disk0:/csco_config/customization.AnyConnect customizations may include custom AnyConnect GUI resources, a binary custom help file and binary VPN scripts, and installer transforms.

Related Commands

Command	Description
revert webvpn AnyConnect-customization	Removes the specified customization object from the flash device of the ASA.
show import webvpn AnyConnect-customization	Lists the customization objects present on the flash device of the ASA.

import webvpn customization

To load a customization object onto the flash device of the ASA, enter the **import webvpn customization** command in privileged EXEC mode.

import webvpn customization *name URL*

Syntax Description

name	The name that identifies the customization object. The maximum number is 64 characters.
URL	Remote path to the source of the XML customization object. The maximum number is 255 characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Make sure WebVPN is enabled on an ASA interface before you enter the **import customization** command. To do so, enter the **show running-config** command.

The ASA does the following when you import a customization object:

- Copies the customization object from the URL to the ASA file system disk0:/csco_config/customization as MD5*name*.
- Performs a basic XML syntax check on the file. If it is invalid, the ASA deletes the file.
- Checks that the file in index.ini contains the record MD5*name*. If not, the ASA adds MD5*name* to the file.
- Copies the MD5*name* file to RAMFS /csco_config/customization/ with as ramfs *name*.

Examples

The following example imports to the ASA a customization object, *General.xml*, from the URL 209.165.201.22/customization and names it *custom1*.

```
ciscoasa# import webvpn customization custom1 tftp://209.165.201.22/customization /General.xml
```

```
Accessing
tftp://209.165.201.22/customization/General.xml...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/custom1...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
329994 bytes copied in 5.350 secs (65998 bytes/sec)
```

Related Commands

Command	Description
revert webvpn customization	Removes the specified customization object from the flash device of the ASA.
show import webvpn customization	Lists the customization objects present on the flash device of the ASA.

import webvpn mst-translation

To load an MST (Microsoft Transform) object onto the flash device of the ASA, enter the **import webvpn mst-translation** command in privileged EXEC mode.

import webvpn mst-transation AnyConnect language *language URL* | **stdin** { *num_chars data* | *data* **quit** } }

Syntax Description

language *language*	The translation language.
stdin {*num_chars data* | *data* **quit**}	Specifies that the data will be provided from stdin. If the number of characters is not specified then the data read from standard input is expected to be base64-encoded followed by "\nquit\n".
URL	Remote path to the source of the XML customization object. The maximum number is 255 characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

This file translates the AnyConnect installer.

Related Commands

Command	Description
show import webvpn mst-translation	Lists the customization objects present on the flash device of the ASA.

import webvpn plug-in protocol

To install a plug-in onto the flash device of the ASA, enter the **import webvpn plug-in protocol** command in privileged EXEC mode.

import webvpn plug-in protocol *protocol URL*

Syntax Description

protocol	• **rdp—**The Remote Desktop Protocol plug-in lets the remote user connect to a computer running Microsoft Terminal Services. Cisco redistributes this plug-in without any changes. The website containing the original is http://properjavardp.sourceforge.net/ . • **ssh,telnet—**The Secure Shell plug-in lets the remote user establish a secure channel to a remote computer, or lets the remote user use Telnet to connect to a remote computer. Cisco redistributes this plug-in without any changes. The website containing the original is http://javassh.org/ . **Caution** The **import webvpn plug-in protocol ssh,telnet** *URL* command installs *both* the SSH and Telnet plug-ins. Do *not* enter this command once for SSH and once for Telnet. When typing the **ssh,telnet** string, do *not* insert a space. Use the **revert webvpn plug-in protocol** command to remove any **import webvpn plug-in protocol** commands that deviate from these requirements. • **vnc—**The Virtual Network Computing plug-in lets the remote user use a monitor, keyboard, and mouse to view and control a computer with remote desktop sharing turned on. Cisco redistributes this plug-in without any changes. The website containing the original is http://www.tightvnc.com/ .
URL	Remote path to the source of the plug-in.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Before installing a plug-in, do the following:

- Make sure Clientless SSL VPN ("webvpn") is enabled on an interface on the ASA. To do so, enter the **show running-config** command.
- Create a temporary directory named "plugins" on a local TFTP server (for example, with the hostname "local_tftp_server"), and download the plug-ins from the Cisco website to the "plugins" directory. Enter the hostname or address of the TFTP server and the path to the plug-in that you need into the URL field of the **import webvpn plug-in protocol** command.

The ASA does the following when you import a plug-in:

- Unpacks the .jar file specified in the *URL*.
- Writes the file to the csco-config/97/plugin directory on the ASA file system.
- Populates the drop-down menu next to the URL attributes in ASDM.
- Enables the plug-in for all future Clientless SSL VPN sessions, and adds a main menu option and an option to the drop-down menu next to the Address field of the portal page. The following table shows the changes to the main menu and address field of the portal page.

Plug-in	Main Menu Option Added to Portal Page	Address Field Option Added to Portal Page
citrix	Citrix Client	citrix://
rdp	Terminal Servers	rdp://
ssh,telnet	SSH	ssh://
	Telnet	telnet://
vnc	VNC Client	vnc://

The ASA does not retain the **import webvpn plug-in protocol** command in the configuration. Instead, it loads the contents of the csco-config/97/plugin directory automatically. A secondary ASA obtains the plug-ins from the primary ASA.

When the user in a Clientless SSL VPN session clicks the associated menu option on the portal page, the portal page displays a window to the interface and displays a help pane. The user can select the protocol displayed in the drop-down menu and enter the URL in the Address field to establish a connection.

Note Support has been added for SSH V2 in addition to previous SSH V1 and Telnet. The plug-in protocol is still the same (ssh and telnet), and the URL formats are as follows:ssh://<target> — uses SSH V2ssh://<target>/?version=1 — uses SSH V1telnet://<target> — uses telnet

To remove the respective **import webvpn plug-in protocol** command and disable support for the protocol, use the **revert webvpn plug-in protocol** command.

Examples

The following command adds Clientless SSL VPN support for RDP:

```
ciscoasa# import webvpn plug-in protocol rdp tftp://209.165.201.22/plugins/rdp-plugin.jar
Accessing
```

```
tftp://209.165.201.22/plugins/rdp-plugin.jar...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/plugin/rdp...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
329994 bytes copied in 5.350 secs (65998 bytes/sec)
```

The following command adds Clientless SSL VPN support for SSH and Telnet:

```
ciscoasa# import webvpn plug-in protocol ssh,telnet
tftp://209.165.201.22/plugins/ssh-plugin.jar
Accessing
tftp://209.165.201.22/plugins/ssh-plugin.jar...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/plugin/ssh...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
238510 bytes copied in 3.650 secs (79503 bytes/sec)
```

The following command adds Clientless SSL VPN support for VNC:

```
ciscoasa# import webvpn plug-in protocol vnc tftp://209.165.201.22/plugins/vnc-plugin.jar
Accessing tftp://209.165.201.22/plugins/vnc-plugin.jar...!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/plugin/vnc...
!!!!!!!!!!!!!!!
58147 bytes copied in 2.40 secs (29073 bytes/sec)
ciscoasa#
```

Related Commands

Command	Description
revert webvpn plug-in protocol	Removes the specified plug-in from the flash device of the ASA.
show import webvpn plug-in	Lists the plug-ins present on the flash device of the ASA.

import webvpn translation-table

To import a translation table used to translate terms displayed to remote users establishing SSL VPN connections, use the **import webvpn translation-table** command in privileged EXEC mode.

import webvpn translation-table *translation_domain* **language** *language url*

Syntax Description

language	Specifies a language for the translation table. Enter the value for *language* in the manner expressed by your browser language options.
translation_domain	Specifies the functional area and associated messages visible to remote users.
url	Specifies the URL of the XML file used to create the customization object.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The ASA provides language translation for the portal and screens displayed to users that initiate browser-based, clientless SSL VPN connections, as well as the user interface displayed to AnyConnect VPN Client users.

Each functional area and its messages that is visible to remote users has its own translation domain and is specified by the *translation_domain argument*. The following table shows the translation domains and the functional areas translated.

Translation Domain	Functional Areas Translated
AnyConnect	*Messages displayed on the user interface of the Cisco AnyConnect VPN Client.*
banners	Banners displayed to remote users and messages when VPN access is denied.
CSD	Messages for the Cisco Secure Desktop (CSD).
customization	*Messages on the login and logout pages, portal page, and all the messages customizable by the user.*

Translation Domain	Functional Areas Translated
plugin-ica	Messages for the Citrix plug-in.
plugin-rdp	Messages for the Remote Desktop Protocol plug-in.
plugin-telnet,ssh	Messages for the Telnet and SSH plug-in.
plugin-vnc	Messages for the VNC plug-in.
PortForwarder	Messages displayed to port forwarding users.
url-list	Text that user specifies for URL bookmarks on the portal page.
webvpn	All the layer 7, AAA, and portal messages that are not customizable.

A translation template is an XML file in the same format as the translation table, but has all the translations empty. The software image package for the ASA includes a template for each domain that is part of the standard functionality. Templates for plug-ins are included with the plug-ins and define their own translation domains. Because you can customize the *login and logout pages, portal page, and URL bookmarks for clientless users,* the ASA **generates the customization** and **url-list** translation domain templates dynamically, and the template automatically reflects your changes to these functional areas.

Download the template for the translation domain using the **export webvpn translation-table** command, make changes to the messages, and use the **import webvpn translation-table** command to create the object. You can view available objects with the **show import webvpn translation-table** command.

Be sure to specify language in the manner expressed by your browser language options. For example, Microsoft Internet Explorer uses the abbreviation >*zh* for the Chinese language. The translation table imported to the ASA must also be named >*zh* .

With the exception of the AnyConnect translation domain, a translation table has no affect, and messages are not translated until you create a customization object, identify a translation table to use in that object, and specify the customization for the group policy or user. Changes to the translation table for the AnyConnect domain are immediately visible to Secure Client users. See the **import webvpn customization** command for more information.

Examples

The following example imports a translation-table for the translation domain affecting the Secure Client user interface, and specifies the translation table is for the Chinese language. The **show import webvpn translation-table** command displays the new object:

```
ciscoasa# import webvpn translation-table anyconnect language zh
tftp://209.165.200.225/anyconnect
ciscoasa# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
ciscoasa# show import webvpn translation-table
Translation Tables' Templates:
customization
AnyConnect
CSD
PortForwarder
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin
```

```
Translation Tables:
zh AnyConnect
```

Related Commands

Command	Description
export webvpn translation-table	Exports a translation table.
import webvpn customization	Imports a customization object that references the translation table.
revert	Removes translation tables from flash.
show import webvpn translation-table	Displays available translation table templates and translation tables.

import webvpn url-list

To load a URL list onto the flash device of the ASA, enter the **import webvpn url-list** command in privileged EXEC mode.

import webvpn url-list *name URL*

Syntax Description

name	The name that identifies the URL list. The maximum number is 64 characters.
URL	Remote path to the source of the URL list. The maximum number is 255 characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Make sure that WebVPN is enabled on a ASA interface before you enter the **import url-list** command. To do so, enter the **show running-config** command.

The ASA does the following when you import a URL list:

- Copies the URL list from the URL to the ASA file system disk0:/csco_config/url-lists as *name on flash* = base 64*name*.
- Performs a basic XML syntax check on the file. If the syntax is invalid, the ASA deletes the file.
- Checks that the file in index.ini contains the record base 64*name*. If not, the ASA adds base 64*name* to the file.
- Copies the *name* file to RAMFS /csco_config/url-lists/ with ramfs name = *name*.

Examples

The following example imports a URL list, *NewList.xml*, from the URL 209.165.201.22/url-lists to the ASA and names it *ABCList*.

```
ciscoasa# import webvpn url-list ABCList tftp://209.165.201.22/url-lists/NewList.xml
```

```
Accessing
tftp://209.165.201.22/url-lists/NewList.xml...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/ABClist...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
329994 bytes copied in 5.350 secs (65998 bytes/sec)
```

Related Commands

Command	Description
revert webvpn url-list	Removes the specified URL list from the flash device of the ASA.
show import webvpn url-list	Lists the URL lists present on the flash device of the ASA.

import webvpn webcontent

To import content to flash memory that is visible to remote Clientless SSL VPN users, use the **import webvpn webcontent** command in privileged EXEC mode.

import webvpn webcontent *destination url source url*

Syntax Description

destination url	**The URL to export to**. The maximum number is 255 characters.
source url	The URL in the ASA flash memory in which the content resides. The maximum number is 64 characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Content imported with the **webcontent** option is visible to remote Clientless users. This includes help content visible on the Clientless portal and logos used by customization objects that customize user screens.

Content imported to URLs with the path /+CSCOE+/ is visible only to authorized users.

Content imported to URLs with the path /+CSCOU+/ is visible to both unauthorized and authorized users.

For example, a corporate logo imported as /+CSCOU+/logo.gif could be used in a portal customization object and be visible on the logon page and the portal page. The same logo.gif file imported as /+CSCOE+/logo.gif would only be visible to remote users after they have logged in successfully.

Help content that appears on the various application screens must be imported to specific URLs. The following table shows the URLs and screen areas for the help content displayed for standard Clientless applications:

URL	Clientless Screen Area
/+CSCOE+/help/*language* /app-access-hlp.inc	Application Access

URL	Clientless Screen Area
/+CSCOE+/help/*language* /file-access-hlp.inc	Browse Networks
/+CSCOE+/help/*language* /net_access_hlp.html	Secure Client
/+CSCOE+/help/*language* /web-access-help.inc	Web Access

The following table shows the URLs and screen areas for the help content displayed for optional plug-in Clientless applications:

URL	Clientless Screen Area
/+CSCOE+/help/*language* /ica-hlp.inc	MetaFrame Access
/+CSCOE+/help/*language* /rdp-hlp.inc	Terminal Servers
/+CSCOE+/help/*language* /ssh,telnet-hlp.inc	Telnet/SSH Servers
/+CSCOE+/help/*language* /vnc-hlp.inc	VNC Connections

The *language* entry in the URL path is the language abbreviation that you designate for the help content. The ASA does not actually translate the file into the language you specify, but labels the file with the language abbreviation.

Examples

The following example imports the HTML file *application_access_help.html,* from a TFTP server at 209.165.200.225, to the URL that stores the Application Access help content in flash memory. The URL includes the abbrevation *en* for the English language:

```
ciscoasa# import webvpn webcontent /+CSCOE+/help/en/app-access-hlp.inc
tftp://209.165.200.225/application_access_help.html
!!!!* Web resource `+CSCOE+/help/en/ap-access-hlp.inc' was successfully initialized
ciscoasa#
```

The following example imports the HTML file *application_access_help.html,* from a tftp server at 209.165.200.225, to the URL that stores the Application Access help content in flash memory. The URL includes the abbrevation *en* for the English language:

```
ciscoasa# import webvpn webcontent /+CSCOE+/help/en/app-access-hlp.inc
tftp://209.165.200.225/application_access_help.html
!!!!* Web resource `+CSCOE+/help/en/ap-access-hlp.inc' was successfully initialized
ciscoasa#
```

Related Commands

Command	Description
export webvpn webcontent	Exports previously imported content visible to Clientless SSL VPN users.
revert webvpn webcontent	Removes content from flash memory.
show import webvpn webcontent	Displays information about imported content.